

**IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE**

**IN RE: HCA HEALTHCARE INC.
DATA SECURITY LITIGATION**

Case No. 3:23-cv-00684

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs RASHEED ABDUL-LATIF, JENNIFER SPERLING, and LESLIE SPERLING (“Plaintiffs”), for themselves and on behalf of all others similarly situated, bring this action against HCA Healthcare, Inc. (“HCA” or “Defendant”). Plaintiffs allege the following based on personal knowledge as to their own acts and on the investigation conducted by their counsel as to all other allegations.

NATURE OF THE ACTION

1. This proposed Class Action is brought by patients of HCA who received health care services at current and former “HCA Healthcare-affiliated hospitals or physician offices” in 20 states, and whose personal data was accessed, exposed, and “made available by an unknown and unauthorized party on an online forum,” as discovered by HCA on or about July 5, 2023 (the “Data Breach”).¹

¹ See *Privacy Update HCA Healthcare Reports Data Security Incident*, July 10, 2023 (<https://web.archive.org/web/20230807123415/https://hcahealthcare.com/about/privacy-update.dot>) (last visited August 15, 2023); *Privacy Update HCA Healthcare Provides Substitute Notice to Certain Patients about a Previously Disclosed Data Security Incident*, August 14, 2023 (last visited August 15, 2023).

2. Patients' data, including those belonging to Patients and Class members which was accessed by unauthorized parties and exposed in this Data Breach includes patients' "Personal Information."² Some "Personal Information" may be categorized either as "Personally Identifiable Information" ("PII") or as "Private Health Information" ("PHI"), or as both PII and PHI. Here, the "Personal Information" accessed and exposed by an unknown and unauthorized party (the "Hacker") includes, patients' names, home postal addresses, zip codes, dates of birth, genders, healthcare service dates, locations of healthcare services, and next healthcare appointment dates.³

3. HCA reported that the Personal Information accessed and exposed in the Data Breach belongs to at least eleven million Class members.⁴

4. The Hacker who accessed Plaintiffs' and Class members' Personal Information in this Data Breach exposed that Personal Information and offered it for sale on a deep web hacking forum.⁵ Such Personal Information is valuable to criminals who can use Personal Information to steal identities and perpetrate numerous fraudulent schemes. Criminals may further use Plaintiffs' Class members' Personal Information to target additional victims for hacking, social engineering, phishing, and other means of stealing information from Plaintiffs, Class members, and others to generate illicit profits.

² See *Privacy Update HCA Healthcare Provides Substitute Notice to Certain Patients about a Previously Disclosed Data Security Incident*, August 14, 2023 (last visited August 15, 2023).

³ *Id.*

⁴ See *id.*

⁵ *DEVELOPING: HCA Healthcare patient data for sale on hacking forum?*, DataBreaches.net, July 5, 2023 (<https://www.databreaches.net/developing-hca-healthcare-patient-data-for-sale-on-hacking-forum/>) (last visited August 15, 2023); *HCA Healthcare releases statement while hacker puts data up for sale on deep web (update1)*, DataBreaches.net, July 10, 2023 (<https://www.databreaches.net/hca-healthcare-releases-statement-while-hacker-puts-data-up-for-sale-on-deep-web/>) (last visited August 15, 2023).

5. HCA, a sophisticated healthcare provider, did not protect Plaintiffs' and Class member's Personal Information.

6. Plaintiffs and Class members are harmed by, and suffer concrete damages from their continuing need to expend their time and financial resources to attempt to mitigate the significantly increased risk of future harm caused by HCA's Data Breach, by their loss of privacy, and by the increased anxiety they will suffer knowing that their Personal Information is at a greatly increased risk of being used by criminals to perpetrate additional crimes against themselves and against others.

7. Plaintiffs and Class members are also injured by the greatly increased risk of future harm that Plaintiffs and Class members suffer as a direct and proximate cause of the Data Breach, such as identity theft and fraud leading to their own credit ratings being damaged, and by their applications for credit and loans.

8. Although HCA advised Plaintiffs and Class members to be "vigilant in identifying calls, emails or SMS texts which appear to be spam or fraudulent" and to "never open links or attachments from untrusted sources," HCA has not notified Plaintiffs and Class any new steps HCA has taken to prevent recurrence of the Data Breach such as remediating vulnerabilities in its IT systems other than disabling "user access to the storage location" from which the Hacker accessed and exposed Plaintiffs' and Class member's Personal Information.

9. While HCA advised that Plaintiffs' and Class members' data was "made available by an unknown and unauthorized party on an online forum," including certain Personal Information, in a list stolen "from an external storage location exclusively used to automate the formatting of email messages," HCA has not stated that this was the extent of the information

stolen,⁶ and indeed, there is reason to believe additional Personal Information was stolen and posted on the deep web, including additional information belonging to one million patients in HCA's San Diego division.⁷

10. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Personal Information was accessed and exposed as a direct result of the Data Breach.

11. Therefore, Plaintiffs bring this proposed Class Action against Defendant HCA to seek redress for HCA's unlawful conduct, asserting claims under common law and under statutory law.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of Class members exceeds 100, many of whom, including Plaintiffs, have different citizenship from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

13. This Court has personal jurisdiction over this action because Defendant maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. See 28 U.S.C. § 1332(a).

⁶ See *HCA Healthcare Reports Data Security Incident*, July 10, 2023 (<https://hcahealthcare.com/about/privacy-update.dot>) (last visited August 8, 2023).

⁷ *HCA Healthcare releases statement while hacker puts data up for sale on deep web (update1)*, DataBreaches.net, July 10, 2023 (<https://www.databreaches.net/hca-healthcare-releases-statement-while-hacker-puts-data-up-for-sale-on-deep-web>) (last visited August 15, 2023).

14. Venue is proper in this Court under 28 U.S.C. § 1391(a) through (d) because Defendant's principal place of business is located in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in, was directed to, and/or emanated from this District.

THE PARTIES

A. Plaintiffs

15. Plaintiffs identified below bring this action on behalf of themselves and others similarly situated in a representative capacity for individuals across the United States. Despite knowing of the substantial cybersecurity risks it faced, HCA, through its actions described herein caused Plaintiffs' valuable Personal Information to be accessed and exposed by unknown and unauthorized criminals, thus causing them harm and continuing increased risk of harm.

16. Based upon counsel's investigation, and upon information and belief, residents of the State of Florida were injured by the Data Breach. The Plaintiffs identified below are also pursuing claims on behalf of citizens and residents of Florida.

17. Plaintiff Jennifer Sperling is citizen and resident of Florida, in the County of Palm Beach, over the age of eighteen. Plaintiff Jennifer Sperling was a patient who provided her Personal Information to HCA to obtain healthcare services at facilities owned and/or managed by HCA prior to HCA's discovery of the Data Breach on or about July 5, 2023.

18. Plaintiff Leslie Sperling is a citizen and resident of Florida, in the County of Palm Beach, over the age of eighteen. Plaintiff Leslie Sperling was a patient who provided his Personal Information to HCA to obtain healthcare services at facilities owned and/or managed by HCA prior to HCA's discovery of the Data Breach on or about July 5, 2023.

19. Based upon counsel's investigation, and upon information and belief, residents of the State of Tennessee were injured by the Data Breach. The Plaintiff identified below is also pursuing claims on behalf of citizens and residents of Tennessee.

20. Plaintiff Rasheed Abdul-Latif is a citizen and resident of Tennessee, in the County of Hamilton, over the age of eighteen. Plaintiff Rasheed Abdul-Latif was a patient who provided his Personal Information to HCA to obtain healthcare services at facilities owned and/or managed by HCA prior to HCA's discovery of the Data Breach on or about July 5, 2023.

B. Defendant

21. Defendant HCA Healthcare, Inc. is a Delaware corporation with its principal place of business located at One Park Plaza, Nashville, Tennessee.⁸ HCA's common stock is publicly traded on the New York Stock Exchange under the trading symbol "HCA."⁹ HCA Healthcare, Inc. was incorporated in Delaware in October 2010.¹⁰ "HCA Healthcare is one of the nation's leading providers of healthcare services comprising 180 hospitals and approximately 2,300 ambulatory sites of care, including surgery centers, freestanding ERs, urgent care centers, and physician clinics, in 20 state and the United Kingdom."¹¹

22. Founded in 1968, "HCA Healthcare is a learning health system that uses its more than 37 million annual patient encounters to advance science, improve patient care and save lives."¹² HCA wrote it "believes the privacy of its patients is a vital part of its mission and remains

⁸ SEC Form 10-K, *Annual Report for the fiscal year ended December 31, 2022*, filed February 17, 2023, HCA Healthcare, Inc., at 3 (<https://d18rn0p25nwr6d.cloudfront.net/CIK-0000860730/17a641c6-2595-460b-8ece-e9aa28cd2237.pdf>) (last visited August 8, 2023).

⁹ *Id.*

¹⁰ *Id.*

¹¹ *HCA Healthcare Reports Data Security Incident*, July 10, 2023, (<https://hcahealthcare.com/about/privacy-update.dot>) (last visited August 8, 2023).

¹² *Id.*

committed to maintaining the security of their personal information.”¹³ HCA’s patients include those whose personal data or “Personal Information,” including “Personally Identifiable Information” (“PII”), or “Protected Health Information” (“PHI”), was compromised in this Data Breach.¹⁴ HCA is a citizen of the state of Tennessee.

FACTUAL ALLEGATIONS

A. HCA, a Sophisticated Healthcare Provider, Collects Patients’ Personal Information including Personal Information and Private Health Information

23. HCA wrote that Defendant is “committed to the care and improvement of human life” and part of HCA’s commitment includes protecting patients’ “Personal Information,” which HCA collects when its patients access HCA’s “Website,” “Portal,” and “Services,” including websites and applications that link to HCA’s “Privacy Policy.”¹⁵

24. HCA collects Personal Information from its patients through the HCA website when patients fill out forms, including from “secure forms,” and also from HCA’s “Web Server Logs,” which captures such information as patients’ internet protocol address, the kind of browser or computer patients use, the number of links the patients click within HCA’s Services, the State or country from which patients access HCA’s services, the date or time patients visit HCA’s Services, the name of the patients’ internet service provider; third party websites the patients link to from HCA’s Services, and from pages or information patients view on HCA’s services; from “Cookies and Web Beacons;” “Geolocation Data” such as patients’ region or postal code.¹⁶

¹³ *Id.*

¹⁴ *See id.*

¹⁵ *See Privacy Policy*, July 1, 2023, (<https://hcahealthcare.com/legal/index.dot#notice-at-collection>) (last visited August 15, 2023.)

¹⁶ *See id.*

25. HCA's Portals collect its patients' Personal Information to allow its patients "private access" to their own medical records, "as well as certain internet-based services" which includes HCA's provision of "assistance in finding a doctor, assistance in scheduling appointments, the ability to register for classes and pre-register for procedures, the ability to make payment for medical services rendered, and access to health and patient education materials and secure messaging...."¹⁷ To access their own medical records, HCA's patients enter Personal Information to the Portal, including their names, email or physical addresses; dates of birth, answers to "secret questions," and "information about patients' location and medical needs to assist in finding a physician, and "may collect and pass on information including health information such as ... patient history" to assist patients "in scheduling appointments, pre-registering for procedures, and registering for classes."¹⁸

26. HCA sends its patients electronic newsletters, notification of account statutes, and marketing communications on a periodic basis in addition to "secure message[s]" sent by doctors.¹⁹

B. HCA Shares its Patients' Personal Information with Authorized Representatives, Healthcare Providers, and Business Partners, including Marketing, Treatment, and Health Care Operations Support Patterners

27. HCA advises its investors that HCA "directly and through [its] vendors and other third parties, collect and store on [HCA's] networks and devices and third-party technology platforms sensitive information including ... personally identifiable information of [HCA's] patients"²⁰

¹⁷ See *id.*

¹⁸ See *id.*

¹⁹ See *id.*

²⁰ SEC Form 10-K, Annual Report for the fiscal year ended December 31, 2022, HCA

28. HCA notes, in a privacy policy accessible through a link at the bottom of its corporate website, that HCA allows access to patients' Personal Information by patients' authorized representatives, those managing accounts on patients' behalf, "for example, a mother managing the account of her son," and those authorized representatives "can view all Personal Information about [the patients] in the Portal."²¹

29. HCA's healthcare providers may also have access to patients' Personal Information for administrative and healthcare services" and HCA "may use Personal Information to respond to and fulfill [patients'] orders and requests."²²

30. HCA allows third party advertising partners to place or recognize unique cookies and web beacons on patients' browsers in order to serve patients targeted messaging and targeted advertisements and to run advertising and marketing campaigns, with HCA's partners' services advertising services, which HCA purports to do in compliance with HIPAA and other applicable laws.²³

31. HCA shares patients' email communications with customer services representatives, employees, medical experts, or agents.²⁴

32. HCA classifies the Personal Information it collects and also lists the Personal Information sells and shares from its Website, Portals, Services, and Offline including "**Identifiers**," e.g., patients' "[r]eal name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's

Healthcare, Inc., filed February 17, 2023, at 38 (<https://d18rn0p25nwr6d.cloudfront.net/CIK-0000860730/17a641c6-2595-460b-8ece-e9aa28cd2237.pdf>) (last visited August 15, 2023).

²¹ *Privacy Policy*, HCA, July 1, 2023, (<https://hcahealthcare.com/legal/index.dot#privacy-policy>) (last visited August 15, 2023).

²² *See id.*

²³ *See id.*

²⁴ *See id.*

license number, and passport number” which HCA discloses “**for a Business Purpose,**” in addition to “**Personal Information categories described in Cal. Civ. Code § 1798.80(e),**” in addition to “**Characteristics of protected classifications under California or under federal law,**” *e.g.*, “[a]ge, race color, ancestry, national origin, citizenship, religion or creed, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, veteran or military statuses, genetic information (including familial genetic information,” “[c]ommercial information,” “[a]udio, electronic, visual, thermal, olfactory or similar information,” “[p]rofessional or employment-related information,” and “[e]ducation information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R Part 99).”²⁵

33. HCA collects other patient data which disclosed for a business purpose and also “[s]old or [s]hared,” *e.g.*, “[g]eolocation data” including region or postal code, and “[i]nternet or [e]lectronic [n]etwork [a]ctivity [i]nformation.”²⁶

34. HCA further describes the following “Sensitive Personal Information” it “Disclosed for a Business Purpose:” “**Personal information that reveals:**” “Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account,” and “Personal information collected and analyzed concerning a consumer’s health.”²⁷

²⁵ *Id.*

²⁶ *Id.*

²⁷ *See id.*

C. HCA Knew of the Risk that Cybercriminals Posed to its Patients' Private Health Information

35. Prior to HCA's purported discovery of the data breach, HCA advised its investors that a "cybersecurity incident or other form of **data breach** could result in the compromise of [HCA's] facilities, confidential data or critical systems" and "give rise to potential harm to patients; remediation and other expenses; and exposure to liability under HIPAA, consumer protection laws, common law theories, or other laws."²⁸

D. HCA had a Responsibility to Safeguard Patients' Personal Information and Private Health Information

36. Prior to HCA's discovery of the Data Breach, HCA advised its investors that the "Health Insurance Portability and Accountability Act of 1996 ('HIPAA') and implementing regulations require the use of uniform electronic data transmission standards and code sets for certain health care claims and payment transactions submitted or received electronically. In addition, HIPAA requires each provider to use a National Provider Identifier."²⁹ HCA continued writing that "the privacy and security regulations promulgated pursuant to HIPAA extensively regulate the use and disclosure of individually identifiable health information, known as 'protected health information,' and require covered entities, including health plans and most health care providers, to implement administrative, physical and technical safeguards to protect the security of such information."

37. HCA further advised its investors that it enforces "compliance in accordance with HIPAA privacy and security regulations" and that HCA's "Information Protection and Security

²⁸ SEC Form 10-K, *Annual Report for the fiscal year ended December 31, 2022*, HCA Healthcare, Inc., filed February 17, 2023, at 38 (<https://d18rn0p25nwr6d.cloudfront.net/CIK-0000860730/17a641c6-2595-460b-8ece-e9aa28cd2237.pdf>) (last visited August 15, 2023) (emphasis added).

²⁹ *Id.* at 23.

Department” monitors HCA’s compliance with HIPAA privacy and security regulations.³⁰ “Violations of the HIPAA privacy and security regulations may result in criminal penalties and in substantial civil penalties per violation.”³¹ The United States Department of Health and Human Services (“HHS”) enforces HIPAA regulations, performs compliance audits and can impose monetary penalties, including for willful neglect.³² State attorneys general are also “authorized to bring civil actions seeking either injunction or damages or damages in response to violations that threaten the privacy of state residents.”³³

38. HCA advised its investors of HCA’s responsibilities to provide notification of Data Breaches concerning “unsecured protected health information to affected individuals,” to provide notification to HHS,” and in large data breaches, to provide notification to the media.³⁴ “Various state laws and regulations may also require [HCA] to notify affected individuals in the event of a data breach involving individually identifiable information.”³⁵

39. HCA advised investors that it is also subject to other federal or state privacy-related laws and regulatory initiatives including the Federal Trade Commission’s (“FTC”) “consumer protection authority which is used to initiate enforcement actions in response to data breaches,” the “California Consumer Privacy Act of 2018 (the ‘CCPA’) which was significantly amended by the California Privacy Rights Act (‘CPRA’), the Colorado Privacy Act, the Utah Privacy Act and the Virginia Consumer Data Protection Act” each of which “afford consumers expanded privacy

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ *Id.*

³⁴ *Id.*

³⁵ *Id.*

protections” including “civil penalties for violations” and under the “CCPA and CPRA” “a private right of action for data breaches.”³⁶

E. HCA Knew it was a Target for Cybersecurity Attacks and Data Breaches and was Vulnerable to Such Attacks

40. HCA advised its investors:

Threats from malicious persons and groups, new vulnerabilities and advanced new attacks against information systems and devices against us or our vendors and other third parties create risk of cybersecurity incidents, including ransomware, malware and phishing incidents. We have seen, and believe we will continue to see, widely spread vulnerabilities that could affect our or other parties’ systems. Mitigation and remediation recommendations continue to evolve, and addressing this and other critical vulnerabilities is a priority for us. The volume and intensity of cyberattacks on hospitals, health systems and other health care entities continue to increase. We are regularly the target of attempted cybersecurity and other threats that could have a security impact, including those by third parties to access, misappropriate or manipulate our information or disrupt our operations, and we expect to continue to experience an increase in cybersecurity threats in the future.³⁷

F. HCA Ignored Government and Industry Guidance, Standards, and Best Practices for Preventing Cybersecurity Attacks and Data Breaches, Causing the Data Breach to Occur

41. The HHS “405(d) Program is a collaborative effort between industry and the federal government to align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector’s

³⁶ *Id.* at 24.

³⁷ *Id.* at 38-39.

cybersecurity posture against cyber threats.”³⁸ It published “*Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP 2023 Edition)*,”³⁹ outlining the top threats facing the HPH Sector” and was providing “small to large” organizations with “recommendations and best practices to prepare and fight against cybersecurity threats that can impact patient safety.”⁴⁰ There, Andrea Palm, Deputy Secretary of Health and Human Resources, advised, “[c]yber-attacks are an increasing threat across all critical infrastructure sectors. For the health sector, cyber-attacks are especially concerning as they can directly threaten not just the security of our systems and information, but also the health and safety of the American public.”⁴¹ Large healthcare organizations “operate in a legal and regulatory environment that is as complicated as their digital ecosystems” including, among others the “Health Insurance Portability and Accountability Act of 1996 (HIPAA)/Health Information Technology for Economic and Clinical Health Act (HITECH) requirements,” “Payment Card Industry Data Security Standard (PCI-DSS1),” “Gramm-Leach-Bliley Act for financial processing,” “General Data Protection Regulation (GDPR) in the European Union,” “Family Educational Rights and Privacy Act (FERPA) for those institutions participating within Higher Education,” “State laws setting standards for privacy and security such as the California Consumer Privacy Act (CCPA),” and “Federal Information Security Modernization Act (FISMA) requirements as incorporated into federal contracts and research grants through agencies such as the National Institutes of Health

³⁸ HHS 405(d) About, (<https://405d.hhs.gov/about>) (last visited August 15, 2023).

³⁹ HICP Main Document (2023 Edition), (<https://405d.hhs.gov/Documents/HICP-Main-508.pdf>) (last visited August 15, 2023); HICP Tech Volume 1 (2023 Edition), (<https://405d.hhs.gov/Documents/tech-vol1-508.pdf>) (last visited August 15, 2023); HICP Tech Volume 2 (2023 Edition), (<https://405d.hhs.gov/Documents/tech-vol2-508.pdf>) (last visited August 8, 2023).

⁴⁰ HHS 405(d) Information, (<https://405d.hhs.gov/information>) (last visited August 15, 2023).

⁴¹ HICP Main Document (2023 Edition) at 2.

(NIH).”⁴² Had HCA complied with HIPAA and other applicable statutes, regulations, and industry standards listed above, and had HCA been properly prepared for cyber-attacks, an unknown and unauthorized party would not accessed and exposed patients’ Personal Information in the Data Breach.

42. HCA is required as a healthcare provider handling patient data to comply with HIPAA Privacy Rule 45 C.F.R. Part 160 and Part 164 Subparts A and E,⁴³ and HIPAA Security Rule 45 C.F.R Part 160 and Part 164 Subparts A and C. Had HCA complied with the aforementioned HIPAA rules, an unknown and unauthorized party would not have accessed and exposed patients’ Personal Information in the Data Breach.

43. HHS Office for Civil Rights (“OCR”) advised HIPAA regulated entities in its “June 2023 OCR Cybersecurity Newsletter,” that “weak or non-existent authentication processes leave your digital door open to intrusion by malicious actors and increases the likelihood of potential compromise of sensitive information – including electronic protected health information (ePHI),” and noted that “86% of attacks to access an organization’s Internet-facing systems (*e.g.*, web server, email servers) used stolen or compromised credentials” and advised “how to best prevent and deter cyber attacks.”⁴⁴ HHS advised that “[e]ffective authentication ensures that only authorized individuals or entities are permitted access to an organization’s information systems,

⁴² *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients*, HHS, at 5-6.

⁴³ See *Privacy Rule Introduction*, HIPAA, ([https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20\(45%20CFR,in%20the%20health%20care%20system\)](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/introduction/index.html#:~:text=The%20Privacy%20Rule%20(45%20CFR,in%20the%20health%20care%20system))) (last visited August 15, 2023); *The Security Rule*, HIPAA, (<https://www.hhs.gov/hipaa/for-professionals/security/index.html#:~:text=The%20Security%20Rule%20requires%20appropriate,and%20C%20of%20Part%20164.>) (last visited August 15, 2023).

⁴⁴ (<https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-june-2023/index.html>) (last visited August 15, 2023).

resources, and data” and that “HIPAA regulated entities are required to implement authentication solutions of sufficient strength to ensure the confidentiality, integrity, and availability of their ePHI.”⁴⁵ Had HCA used effective authentication, an unknown and unauthorized party would not have been able to access and expose patients’ Personal Information in the Data Breach.

44. The FTC published several guides advising businesses on how to protection personal information including *Start with Security: A Guide for Business*,⁴⁶ *Stick with Security*,⁴⁷ *Protecting Personal Information: A Guide for Business*,⁴⁸ and *Data Breach Response: A Guide for Business*.⁴⁹ Had HCA followed FTC guidance, an unknown and unauthorized party would not have accessed and exposed patients’ Personal Information in the Data Breach.

45. Further, HCA has a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15. U.S.C. § 45 (“FTCA”), which prohibits “unfair practices in or affecting commerce,” including the unfair practice of failing to use reasonable measures to protect confidential data. Had HCA complied with the FTCA, an unknown and unauthorized party would not have accessed and exposed patients’ Personal Information in the Data Breach.

46. The FBI’s Internet Crime Complaint Center (“IC3”) has received over seven million complaints regarding cyber matters such as online fraud, hacking, extortion, and identity

⁴⁵ *Id.*

⁴⁶ June 2015 (<https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>) (last visited August 15, 2023).

⁴⁷ Thomas B. Pahl, Acting Director, FTC Bureau of Consumer Protection, July 28, 2017 (<https://www.ftc.gov/business-guidance/blog/2017/07/start-security-and-stick-it>) (last visited August 15, 2023).

⁴⁸ October 2016 (https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited August 15, 2023).

⁴⁹ February 2021 (https://www.ftc.gov/system/files/documents/plain-language/560a_data_breach_response_guide_for_business.pdf) (last visited August 15, 2023).

theft since IC3's inception in May 2000.⁵⁰ IC3 aggregates submitted data to produce "an annual report on trends impacting the public as well as routinely providing intelligence reports about trends."⁵¹ Out of the 870 complaints IC3 received in 2022 indicating that organizations belonging to a critical infrastructure sector were victims of ransomware cybersecurity attacks, "Healthcare and Public Health" had the most complaints of any industry at 210.⁵² Had HCA reacted to the FBI's warning of the risk of cybersecurity attacks in a responsible manner, an unknown and unauthorized party would not have accessed and exposed patients' Personal Information in the Data Breach.

47. Health-ISAC, the "Health Information Sharing and Analysis Center," is "a trusted community of critical infrastructure owners and operators within the Health and Public Health sector (HPH)" "primarily focused on sharing timely, actionable and relevant information with each other including intelligence on threats, incidents and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable material."⁵³ HCA is a member of the Health-ISAC community and HCA's Director of CyberSecurity – Information Protection and Security is a member of the Health-ISAC Board of Directors.⁵⁴ In August 2022, Health-ISAC published a white paper, *Identity and Zero Trust: A Health-ISAC Guide for CISOS*, which advised readers to use multi-factor authentication ("MFA"), employ "fine-grained authorization," and

⁵⁰ 2022 Internet Crime Report, FBI Internet Crime Complaint Center at 4, (https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf) (last visited August 15, 2023).

⁵¹ *Id.*

⁵² *Id.* at 14.

⁵³ Health-ISAC Frequently Asked Questions, (<https://h-isac.org/h-isac-faq/>) (last accessed August 15, 2023).

⁵⁴ Health-ISAC Board of Directors, (<https://h-isac.org/h-isac-board/>) (last visited August 8, 2023).

explained the importance of “[s]ecuring all communication,” in addition to “[m]onitoring the integrity and security of all owned assets, the network and communication,” [g]ranting access on a per session basis,” “[c]reating policy-based authorization that is based on contextual information – e.g., what device are you logging in from, geolocation, and other behavioral and environmental attributes,” and “[a]dding devices to the target system and resources.”⁵⁵ Had HCA heeded Health-ISAC’s advice, best practices, and mitigation strategies, including employing MFA and fine-grained access controls, an unknown and unauthorized party would not have accessed and exposed patients’ Personal Information in the Data Breach.

G. HCA Ignored its Own Information Security Policies, Causing the Data Breach to Occur

48. HCA maintains numerous corporate policies and procedures regarding Information Protection and Security including *IP.SEC.001 Information Security – Program Requirements Policy*, which established “general, high level requirements” for HCA while “Information Security Standards ... support these high-level requirements.” Policy statements are organized based on an industry standard framework (ISO 27002)” and one or more ‘Information Security Standards supports each policy statement,”⁵⁶ *IP.SEC.001*, mandates that HCA’s [o]perating systems and applications must be configured to provide secure login and authorization mechanisms in order to authenticate user identity and validate access for appropriateness before permitting access to systems that store, process, or transmit Sensitive or Restricted Data. Access to information and applications must be restricted to authorized users.” If HCA had complied with its own policies,

⁵⁵ (https://h-isac.org/wp-content/uploads/2022/08/H-ISAC_White-Paper-ZeroTrust_FINAL_82522.pdf) (last visited August 15, 2023).

⁵⁶ *Summary of Policies and Procedures: Updated on June 8, 2022*, (<https://hcahealthcare.com/util/forms/ethics/2022-jul-summary-a.pdf> at 25) (last visited August 15, 2023).

an unknown and unauthorized party would not have accessed and exposed patients' Personal Information in the Data Breach.

H. HCA's Failure to Follow Government and Industry Standards and its Own Information Security Policy Resulted in a Data Breach where an Unknown and Unauthorized Party Accessed and Exposed Plaintiffs' and Class members' Personal Information

49. On July 5, 2023, a website specializing in data breaches, "DataBreaches.net" ("DataBreaches") reported a "new user on a hacking forum" listed "patient data from HCA Healthcare ... for sale."⁵⁷ The seller wrote, "[a]s of 2021, HCA healthcare is ranked #62 on the Fortune 500 rankings of the largest United States corporations by total revenue." "Data is grouped by division into 17 files totaling to 27,700,000 rows. More data is included in the sale. HCA Healthcare have until 10th to meet the demands." The seller wrote, "2020-2023" "sample 1/4 27,700,000" and listed field headers for the sample: "Encounter_Id|Person_DW_Id|EMPI_Text|MRec_dt|First_Name|Last_Name|City|State|Zip_code|Phone|Decade|Email_Address|Date_of_Birth|Birthday_Month|Patient_Age_Months|Gender|Coid|Coid_Name|Division|Facility_DW_Id|Facility_Name|Next_Appt_Date|Next_Appt_Booked_Date|Tokenized_Campaign|Source_System_Name|MHO_Id."⁵⁸

HCA did not reply immediately to an email from DataBreaches asking if HCA "had experienced a breach" and if HCA was aware that data allegedly from HCA "was up for sale on a hacking forum."⁵⁹ DataBreaches updated its report included the news that the seller told

⁵⁷ *DEVELOPING: HCA Healthcare patient data for sale on hacking forum?*, DataBreaches.Net, July 5, 2023, (<https://www.databreaches.net/developing-hca-healthcare-patient-data-for-sale-on-hacking-forum/>) (last visited August 15, 2023)

⁵⁸ *Id.*

⁵⁹ *Id.*

DataBreaches that the seller was also the hacker, and that the seller/hacker contacted HCA on July 4 to make contact.” DataBreaches did not know if HCA responded to the hacker.⁶⁰

50. On July 10, 2023, DataBreaches reported it was in continued contact with the seller/hacker who explained “that this was a hack not a leak” and the seller/hacker had contacted HCA Healthcare on July 4 and given HCA until July 10 to respond to demands. HCA did not reply to DataBreaches’ inquiries at the time but later told a third party that “the emails had been caught up in some DMARC-related filter.”⁶¹ DataBreaches quoted from HCA’s July 10, 2023 Press Release that HCA “recently discovered that a list of certain information with respect to some of its patients was made available by an unknown and unauthorized party on an online forum” where the list includes patients’ “name, city, and zip code;” “email, telephone number, date of birth, gender;” and “service date location, and next appointment date,” and that the list contained information used for email messages but that HCA did not believe that “clinical information such as treatment, diagnosis, or condition)” was involved, though the hacker wrote DataBreaches, “**I have emails with health diagnosis that correspond to a ClientID.**”⁶²

Further, HCA reported “that the incident appears to be a theft from an external storage location ‘exclusively used to automate the formatting of email messages.’”⁶³ DataBreaches quoted from HCA’s July 10, 2023 Privacy Update and questioned the veracity of HCA’s statements as to the number of patients with accessed and exposed Personal Information, noting that while HCA wrote that it believed the list contained “approximately 27 million rows of data that may include

⁶⁰ *Id.*

⁶¹ *HCA Healthcare releases statement while hacker puts data up for sale on deep web (update1)*, DataBreaches.Net, July 10, 2023, (<https://www.databreaches.net/hca-healthcare-releases-statement-while-hacker-puts-data-up-for-sale-on-deep-web/>) (last accessed August 8, 2023).

⁶² *Id.*

⁶³ *Id.*

information for approximately 11 million HCA Healthcare patients,” HCA did not claim that the hacker/seller acquired no other information. DataBreaches reported, in fact that the hacker/seller wrote, referring to HCA, “They claim ‘11 Million’ not like they would know, they lost all their data.” The hacker/seller uploaded a second sample of data on July 9, 2023, including “1 million records seemingly form the San Antonio Division, where each record was one patient.” Had HCA taken reasonable and adequate precautions to safeguard its patient’s data it would not have been accessed and exposed by the hacker/seller. Further, had HCA provided prompt adequate notice to its patients whose data was accessed and exposed by the hacker/seller, patients would have been able to mitigate damages caused by HCA’s Data Breach.

I. Plaintiffs’ and Class members’ Personal Information Including PHI Are Valuable

51. According to HHS and the “Healthcare & Public Health Sector Council,” “[h]ealthcare records continue to be one of the most lucrative items on the underground market, ranging from \$250 to \$1,000 compared to other items like credit cards only selling for an average \$100. This demonstrates the value of data like Protected Health Information (PHI) to cyber-attackers and their motivation for attacking healthcare institutions. Therefore, protecting a patient’s health information and PHI is paramount at every level of an organization, from practitioners to executives.”⁶⁴

52. As a sophisticated healthcare provider, HCA knew it subjected itself to HIPAA requirements to comply with provisions designed to protect the privacy of patients’ valuable Personal Information including PHI.

⁶⁴ *Id.*

53. As a sophisticated business engaged in the collection, distribution, sharing, and sale of consumers' Personal Information, HCA knew it subjected itself to FTC requirements to comply with provisions designed to protect the privacy of consumer's Personal Information.

54. HCA knew or should have known that its patient's Personal Information, including PII and PHI is valuable, and therefore a prime target for criminals. HCA should have taken adequate steps to protect that Personal Information from Data Breaches.

55. HCA failed to take reasonable and adequate steps to prevent patients' Personal Information from being accessed by an unknown and unauthorized party and exposed in the Data Breach.

J. Plaintiffs' Experiences

1. Jennifer Sperling

56. Plaintiff Jennifer Sperling sought and obtained healthcare services from Defendant at a healthcare facility known as HCA Florida Atlantis Orthopedics, located in West Palm Beach, Florida within the last three years.

57. Plaintiff sought and obtained healthcare services from Defendant at a healthcare facility known as HCA Florida Palm Beach Gastroenterology, located in West Palm Beach, Florida, within the last three years.

58. Plaintiff sought and obtained healthcare services from Defendant at healthcare facility known as Palms West Surgicenter located in Loxahatchee, Florida, within the last three years.

59. Plaintiff's Personal Information was collected by HCA in order for HCA to provide healthcare to Plaintiff.

60. Plaintiff received an email notice from Defendant HCA on or about July 16, 2023 (the “Notice”), advising that Personal Information belonging to Defendant’s “patients was made available by an unknown and unauthorized party on an online forum,”⁶⁵ indicating that Plaintiff’s Personal Information was among the information accessed without authorization during the Data Breach and that said information was further exposed on a hacking forum on the Deep Web. HCA listed categories of Personal Information accessed and exposed by the unknown and unauthorized party and advised Plaintiff to “remain vigilant about any suspicious or unexpected communications from anyone claiming to be affiliated with HCA Healthcare,” specifically “any communication regarding an invoice, outstanding balance, or payment reminder” that Plaintiff was “not expecting” or “believe[s] to be fraudulent,” so HCA could “confirm the legitimacy of the message.”⁶⁶ Upon receiving the notice, Plaintiff took steps to protect her Personal Information such as carefully examining unexpected emails for authenticity upon receipt and reviewed bank account and financial statements for suspicious charges.

61. As a result of HCA’s Data Breach, Plaintiff was harmed by receiving a significant increase in spam and phishing emails and must expend time to review the emails and determine if the emails are legitimate.

62. HCA’s Data Breach has caused Plaintiff to experience increased anxiety and to suffer emotional distress due to Plaintiff’s loss of privacy and due to Plaintiffs’ increased risk of criminals exploiting Plaintiff’s Personal Information to commit additional crimes including fraud and identity theft against Plaintiff. Criminals perpetrate fraud and identity theft through such

⁶⁵ HCA Data Breach email notice, received by Plaintiff Jennifer Sperling on or about July 16, 2023, attached as Exhibit A.

⁶⁶ *Id.*

means as sending a great number of illegitimate phishing emails which are often designed to access consumers' systems and steal consumers' financial information.

63. Plaintiff has also suffered emotional distress given Plaintiffs' increased risk of further harm given the exposure of Plaintiff's Personal Information resulting from Defendant's failure to adequately secure and protect Plaintiff's Personal Information. Criminals steal Personal Information to perpetrate further crimes including identity theft and fraud. HCA's exposure of Plaintiffs' Personal Information directly harmed Plaintiff by greatly increasing the risk of becoming a victim of identity theft or fraud.

64. HCA also harmed Plaintiff through causing Plaintiff to spend time mitigating the additional imminent harm that is at a greatly increased risk of occurring through the actions of criminals who were able to access Plaintiff's exposed Personal Information as a direct and proximate result of HCA's Data Breach.

65. Plaintiff is further harmed by the increased risk of her being a victim of future data breaches at HCA. HCA has not provided any indication that it has taken adequate and reasonable steps to further protect its network, systems, or email servers from unauthorized access by unknown users, other than preventing user access to a particular email server from which a list of Plaintiff's personal information was accessed by an unknown and unauthorized party and exposed in this Data Breach.

66. HCA's delay in providing Plaintiff with necessary information to protect herself from the imminent risk of fraud and other crimes resulting from the Data Breach causes further harm to Plaintiff.

67. HCA's failure to take reasonable action to adequately mitigate the risk of future data breaches at HCA from occurring causes further harm to Plaintiff.

68. HCA further harmed Plaintiff by failing to provide adequate and timely notice to Plaintiff such as would allow Plaintiff to act to mitigate the greatly increased risk of fraud and data theft caused by the Data Breach.

2. ***Leslie Sperling***

69. Plaintiff Leslie Sperling sought and obtained healthcare services from Defendant at a healthcare facility known as HCA Florida JFK Hospital, located in Atlantis, Florida, within the last three years.

70. Plaintiff sought and obtained healthcare services from Defendant at a healthcare facility known as HCA Florida JFK Primary Care Center, located in Atlantis, Florida, within the last three years.

71. Plaintiff sought and obtained healthcare services from Defendant at a healthcare facility known as Palms West Surgicenter, located in Loxahatchee, Florida, within the last three years.

72. Plaintiff's Personal Information was collected by HCA in order for HCA to provide healthcare to Plaintiff.

73. Plaintiff received an email notice from Defendant HCA on or about July 16, 2023 (the "Notice"), advising that Personal Information belonging to Defendant's "patients was made available by an unknown and unauthorized party on an online forum,"⁶⁷ indicating that Plaintiff's Personal Information was among the information accessed without authorization during the Data Breach and that said information was further exposed on a hacking forum on the Deep Web. HCA listed categories of Personal Information accessed and exposed by the unknown and unauthorized

⁶⁷ HCA Data Breach email notice, received by Plaintiff Jennifer Sperling on or about July 16, 2023, attached as Exhibit A.

party and advised Plaintiff to “remain vigilant about any suspicious or unexpected communications from anyone claiming to be affiliated with HCA Healthcare,” specifically “any communication regarding an invoice, outstanding balance, or payment reminder” that Plaintiff was “not expecting” or “believe[s] to be fraudulent,” so HCA could “confirm the legitimacy of the message.”⁶⁸ Upon receiving the notice, Plaintiff took steps to protect his Personal Information such as carefully examining the Notice for authenticity, examined unexpected emails for authenticity upon receipt, and reviewed bank account and financial statements for suspicious charges.

74. As a result of HCA’s Data Breach, Plaintiff was harmed by receiving a significant increase in spam and phishing emails and must expend time to review the emails and determine if the emails are legitimate.

75. HCA’s Data Breach has caused Plaintiff to experience increased anxiety and to suffer emotional distress due to Plaintiff’s loss of privacy and due to Plaintiffs’ increased risk of criminals exploiting Plaintiff’s Personal Information to commit additional crimes including fraud and identity theft against Plaintiff. Criminals perpetrate fraud and identity theft through such means as sending a great number of illegitimate phishing emails which are often designed to access consumers’ systems and steal consumers’ financial information.

76. Plaintiff has also suffered emotional distress given Plaintiffs’ increased risk of further harm given the exposure of Plaintiff’s Personal Information resulting from HCA’s failure to adequately secure and protect Plaintiff’s Personal Information. Criminals steal Personal Information to perpetrate further crimes including identity theft and fraud. HCA’s exposure of Plaintiffs’ Personal Information directly harmed Plaintiffs by greatly increasing the risk of becoming a victim of identity theft or fraud.

⁶⁸ *Id.*

77. HCA also harmed Plaintiff through causing Plaintiff to spend time mitigating the additional imminent harm that is at a greatly increased risk of occurring through the actions of criminals who were able to access Plaintiff's exposed Personal Information as a direct and proximate result of HCA's Data Breach.

78. Plaintiff is further harmed by the increased risk of their being a victim of future data breaches at HCA. HCA has not provided any indication that it has taken adequate and reasonable steps to further protect its network, systems, or email servers from unauthorized access by unknown users, other than preventing user access to a particular email server from which a list of Plaintiff's Personal Information was accessed and exposed in this Data Breach.

79. HCA's delay in providing Plaintiff with necessary information to protect themselves from the imminent risk of fraud and other crimes resulting from the Data Breach causes further harm to Plaintiff.

80. HCA's failure to take reasonable action to adequately mitigate the risk of future data breaches at HCA from occurring causes further harm to Plaintiff.

81. HCA further harmed Plaintiff by failing to provide adequate and timely notice to Plaintiff such as would allow Plaintiff to act to mitigate the greatly increased risk of fraud and data theft caused by the Data Breach

3. ***Rasheed Abdul-Latif***

82. Plaintiff Rasheed Abdul-Latif sought and obtained healthcare services from Defendant at Parkridge East Hospital, located in Chattanooga, Tennessee, within the last three years.

83. Plaintiff received an email notice from Defendant HCA on or about July 16, 2023 (the "Notice"), advising that Personal Information belonging to Defendant's "patients was made

available by an unknown and unauthorized party on an online forum,”⁶⁹ indicating that Plaintiff’s Personal Information was among the information accessed without authorization during the Data Breach and that said information was further exposed on a hacking forum on the Deep Web. HCA listed categories of Personal Information accessed and exposed by the unknown and unauthorized party and advised Plaintiff to “remain vigilant about any suspicious or unexpected communications from anyone claiming to be affiliated with HCA Healthcare,” specifically “any communication regarding an invoice, outstanding balance, or payment reminder” that Plaintiff was “not expecting” or “believe[s] to be fraudulent,” so HCA could “confirm the legitimacy of the message.”⁷⁰ Upon receiving the notice, Plaintiff took steps to protect his Personal Information such as carefully examining the Notice for authenticity, examined unexpected emails for authenticity upon receipt, and reviewed bank account and financial statements for suspicious charges.

84. As a result of HCA’s Data Breach, Plaintiff was harmed by receiving a significant increase in spam and phishing emails and must expend time to review the emails and determine if the emails are legitimate.

85. HCA’s Data Breach has caused Plaintiff to experience increased anxiety and to suffer emotional distress due to Plaintiff’s loss of privacy and due to Plaintiffs’ increased risk of criminals exploiting Plaintiff’s Personal Information to commit additional crimes including fraud and identity theft against Plaintiff. Criminals perpetrate fraud and identity theft through such means as sending a great number of illegitimate phishing emails which are often designed to access consumers’ systems and steal consumers’ financial information.

⁶⁹ HCA Data Breach email notice, received by Plaintiff Jennifer Sperling on or about July 16, 2023, attached as Exhibit A.

⁷⁰ *Id.*

86. Plaintiff has also suffered emotional distress given Plaintiffs' increased risk of further harm given the exposure of Plaintiff's Personal Information resulting from HCA's failure to adequately secure and protect Plaintiff's Personal Information. Criminals steal Personal Information to perpetrate further crimes including identity theft and fraud. HCA's exposure of Plaintiffs' Personal Information directly harmed Plaintiffs by greatly increasing the risk of becoming a victim of identity theft or fraud.

87. HCA also harmed Plaintiff through causing Plaintiff to spend time mitigating the additional imminent harm that is at a greatly increased risk of occurring through the actions of criminals who were able to access Plaintiff's exposed Personal Information as a direct and proximate result of HCA's Data Breach.

88. Plaintiff is further harmed by the increased risk of their being a victim of future data breaches at HCA. HCA has not provided any indication that it has taken adequate and reasonable steps to further protect its network, systems, or email servers from unauthorized access by unknown users, other than preventing user access to a particular email server from which a list of Plaintiff's Personal Information was accessed and exposed in this Data Breach.

89. HCA's delay in providing Plaintiff with necessary information to protect themselves himself from the imminent risk of fraud and other crimes resulting from the Data Breach causes further harm to Plaintiff.

90. HCA's failure to take reasonable action to adequately mitigate the risk of future data breaches at HCA from occurring causes further harm to Plaintiff.

91. HCA further harmed Plaintiff by failing to provide adequate and timely notice to Plaintiff such as would allow Plaintiff to act to mitigate the greatly increased risk of fraud and data theft caused by the Data Breach.

CLASS ACTION ALLEGATIONS

92. Plaintiffs bring this lawsuit as a prospective class action on behalf of themselves and all others similarly situated as members of the proposed Classes pursuant to Federal Rules of Civil Procedure 23(a), 23(b)(2), (b)(3) and (c)(4). As described below, this action satisfies the numerosity, commonality, typicality, adequacy, predominance, and superiority requirements of Rules 23(a) and 23(b)(3). This action also satisfies the requirements of Rules 23(b)(2) and (c)(4).

93. Pursuant to Fed. R. Civ. Proc. 23(a) and (b)(2), (b)(3) and/or (c)(4), Plaintiffs assert classes based on the applicable state law of the plaintiffs. The Class and Subclasses are defined as:

94. **Nationwide Class:** All individuals residing in the United States whose Personal Information including Personally Identifiable Information and/or Protected Health Information was accessed by an unknown and unauthorized party and exposed as a result of the Data Breach.

95. **Florida Subclass:** All those who residing in the State of Florida whose Personal Information including Personally Identifiable Information and/or Protected Health Information was accessed by an unknown and unauthorized party and exposed as a result of the Data Breach.

96. **Tennessee Subclass:** All those who residing in the State of Tennessee whose Personal Information including Personally Identifiable Information and/or Protected Health Information was accessed by an unknown and unauthorized party and exposed as a result of the Data Breach.

97. Excluded from the Class and Tennessee Subclass and Florida Subclass (the “Subclasses”) are (1) Defendant, any entity or division in which Defendant has a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge’s staff; (3) any Judge sitting in the presiding state

and/or federal court system who may hear an appeal of any judgment entered; and (4) those persons who have suffered personal injuries as a result of the facts alleged herein. Plaintiffs reserve the right to amend the Class and Subclass definitions if discovery and further investigation reveal that the Class or any Subclass should be expanded or otherwise modified.

98. **Numerosity under Federal Rule of Civil Procedure 23(a)(1).** Although the exact number of Class members is uncertain and can only be ascertained through appropriate discovery, upon information and belief, this Class consists of millions of individuals whose Personal Information was accessed and exposed in the Data Breach, a number great enough such that joinder is impracticable. The Class members are readily identifiable from information and records in HCA's custody and control.

99. **Commonality under Federal Rule of Civil Procedure 23(a)(2).** There are questions of law and fact common to Plaintiffs and Class members, which predominate over any questions affecting only individual Class members. These common questions of law and fact include, without limitation:

- a. Whether HCA unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class members' Personal Information;
- b. Whether HCA failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information accessed by an unknown and unauthorized party and exposed in the Data Breach;
- c. Whether HCA truthfully represented the nature of its security systems, including their vulnerability to hackers;

- d. Whether HCA's data security programs prior to and during the Data Breach complied with applicable data security laws and regulations, *e.g.*, HIPAA and the FTCA;
- e. Whether HCA's data security programs prior to and during the Data Breach were consistent with healthcare industry standards;
- f. Whether HCA owed a duty to Class members to safeguard their Personal Information;
- g. Whether HCA breached its duty to Class members to safeguard their Personal Information;
- h. Whether criminals, *e.g.*, hackers, obtained, sold, copied, stored or released Class members' Personal Information;
- i. Whether HCA knew or should have known that its data security programs and monitoring processes were deficient;
- j. Whether Class members suffered legally cognizable damages as a result of HCA's misconduct;
- k. Whether HCA's conduct was negligent;
- l. Whether HCA's conduct was negligent *per se*;
- m. Whether HCA's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;
- n. Whether HCA breached express contracts with Plaintiffs and Class members;
- o. Whether HCA breached implied contracts with Plaintiffs and Class members;
- p. Whether HCA was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class members;

- q. Whether HCA invaded the Privacy of Plaintiffs and Class members;
- r. Whether HCA failed to provide accurate and complete notice of the Data Breach in a timely manner; and
- s. Whether the Class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

100. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of those of the Class members because Plaintiffs' Personal Information, like that of every Class member, was accessed and exposed in the Data Breach.

101. **Adequacy of Representation under Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

102. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** HCA has engaged in a common course of conduct toward Plaintiffs and the Class members, in that all Plaintiffs' and the Class members' data at issue here was stored by HCA and accessed and exposed during the Data Breach. The common issues arising from HCA's conduct affecting Class members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

103. **Superiority under Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of

inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for HCA. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

104. **Declaratory and Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2).** HCA has acted on grounds that apply generally to the Plaintiffs and the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis. HCA failed to take actions to safeguard Plaintiffs' and Class members' Personal Information such that injunctive relief is appropriate and necessary.

105. **Issue Certification Appropriate under Federal Rule of Civil Procedure 23(c)(4).** In the alternative, this litigation can be brought and maintained a class action with respect to particular issues, such as 'CA's liability with respect to the foregoing causes of action

CAUSES OF ACTION

106. Plaintiffs bring these causes of action on behalf of the Nationwide Class, the Florida Subclass, and the Tennessee Subclass, as defined herein.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1: NEGLIGENCE

On behalf of Plaintiffs and the Nationwide Class

107. Plaintiffs incorporate by reference and re-allege the allegations contained in all preceding paragraphs of this Complaint.

108. HCA required Plaintiffs and Class members to submit non-public, Personal Information in order to receive healthcare from HCA, its subsidiaries, and its affiliates.

109. In providing their Personal Information, Plaintiffs and Class members had a reasonable expectation that their Personal Information, including PII and PHI, would be securely maintained and not easily accessible to, or exposed by criminals.

110. Plaintiffs and Class members had a reasonable expectation that in the event of a data breach, HCA would provide timely and adequate notice to them, to HHS, and would properly identify what Personal Information was exposed during a data breach so that Plaintiffs, Class and Subclass members could take prompt and appropriate steps to safeguard their identities.

111. HCA had a duty as a healthcare provider to employ reasonable security measures to Plaintiffs' and Class and Subclass members' patient data under HIPAA Privacy Rule 45 C.F.R. Part 160 and Part 164 Subparts A and E, and under HIPAA Security Rule 45 C.F.R Part 160 and Part 164 Subparts A and C.

112. HCA had a duty to employ reasonable security measures to Protect Plaintiffs' Class and Subclass members' data under Section 5 of the Federal Trade Commission Act, 15. U.S.C. § 45 ("FTCA"), which prohibits "unfair practices in or affecting commerce," including the unfair practice of failing to use reasonable measures to protect confidential data.

113. HCA, as a company that collects sensitive Personal Information, including PII and PHI, from consumers and patients and likewise stores, maintains, distributes, shares, and sells that data for profit, has a contractual duty to protect that Personal Information and in the event of a Data Breach, to promptly and to adequately notify Plaintiffs and Class members that their Personal Information has been accessed by an unknown and unauthorized party and exposed on a hacking forum.

114. HCA, as a healthcare company that collects sensitive Personal Information from consumers and patients such as Plaintiffs and Class members, and likewise stores, maintains,

distributes, shares, and sells that data for profit, has a duty arising independently from any contract to protect that information and in the event of a Data Breach, to promptly and adequately notify Plaintiffs and Class members.

115. HCA, as a company that purports to believe that the privacy of its patients is a vital part of its mission and remains committed to maintaining the security of their Personal Information owed a duty of care Plaintiffs and Class members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, including email servers, and the personnel responsible for them, adequately protected and safeguarded the Personal information of the Plaintiffs and the Class members.

116. Likewise, as the collector and keeper of Plaintiffs and Class members' Personal Information, HCA had a special duty to of Plaintiffs and Class members to promptly and adequately provide notice of the Data Breach so as to allow Plaintiffs and Class members to take prompt and appropriate steps to safeguard their Personal Information, their identities, and their credit.

117. HCA had a common law duty to prevent foreseeable harm to others. Plaintiffs and Class members were the foreseeable and probable victims of its inadequate security practices. It was foreseeable that Plaintiffs and Class members would be harmed by HCA's failure to protect their Personal Information because hackers are known to routinely attempt to steal such information and use it for criminal purposes.

118. HCA knew or should have known that the Plaintiffs, and Class members were relying on HCA to adequately safeguard and maintain their Personal Information.

119. HCA publicly acknowledged Plaintiffs and Class members' reliance on HCA's duty to safeguard their Personal Information in its 2022 annual report.

120. HCA breached its duties, and thus was negligent, by failing to use reasonable measures to protect the Plaintiffs' and Class members' data. The specific negligent acts and omissions committed by HCA include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Personal Information;
- b. Failing to adequately monitor the security of its network, systems and email servers;
- c. Failing to ensure that its email system had policies and procedures in place to maintain and protect information in accordance with reasonable information security standards;
- d. Failing to have in place policies and procedures to mitigate the harm caused by a Data Breach;
- e. Failing to detect in a timely manner that Class member's Personal Information had been accessed by an unknown authorized party and exposed on a deep web forum;
- f. Failing to timely notify Class members about the Data Breach so Class members could take appropriate steps to promptly mitigate the potential for additional injuries such as fraud, identity theft, and other damages.

121. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT 2: NEGLIGENCE PER SE
On behalf of Plaintiffs and the Nationwide Class

122. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-106 of this Complaint.

123. In addition to the common law and special relationship duties alleged herein, HCA also owed a duty to safeguard Plaintiffs' and Class members' Personal Information by statute.

124. HCA's duty of care to use reasonably security measures arose as a result of the special relationship that existed between HCA and consumers, recognized by laws and regulations, including, but not limited to HIPAA, the FTC Act, and common law. HCA was best positioned to ensure its network and systems were sufficiently secure to protect against the foreseeable risk of harm to Plaintiffs, Class and Subclass members from a data breach.

125. HCA's duty to use reasonably security measures to protect patient's Personal Information including PHI under HIPAA required HCA implement administrative, physical and technical safeguards to protect the security of such information in accordance with 45 C.F.R. Parts 160, 164.

126. HCA's duty to use reasonable security measures to protect consumer's confidential information arises under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), which prohibits "unfair practices in or affecting commerce," including the unfair practice of failing to use reasonable measures to protect confidential data.

127. HCA's duty to use reasonable care in protecting Personal Information arose not only as a result of the statutes and regulations described above, but also because HCA is bound by industry standards to protect confidential Personal Information.

128. HCA breached that duty, which, as discussed herein, caused Plaintiffs and Class members injuries, for which they are entitled to damages.

129. As a direct and proximate result of HCA's negligent conduct, Plaintiffs and Class members have suffered injuries and are entitled to nominal, compensatory, consequential and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT 3: GROSS NEGLIGENCE

On behalf of Plaintiffs and the Nationwide Class

130. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-106 of this Complaint.

131. HCA knew that it was protecting the most sensitive Personal Information about Plaintiffs and Class members that exists, i.e., healthcare information, which can impact any area of an individual's life, e.g., housing, employment, benefits, and education.

132. HCA's failure to keep this Personal Information, including PII and PHI, safe was grossly negligent, as HCA was aware of the grave consequences of not keeping this Personal Information secure.

133. As a result of Defendant's gross negligence, Plaintiffs and Class members have suffered injury and are entitled to nominal, compensatory, consequential, and all other damages which the Court deems appropriate in an amount to be proven at trial.

COUNT 5: BREACH OF EXPRESS CONTRACT

On behalf of Plaintiffs and the Nationwide Class

134. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-106 of this Complaint.

135. HCA acquired and maintained the Plaintiffs' and Class members' Personal Information that HCA received directly through HCA's healthcare providers.

136. HCA made express promises to Plaintiffs and Class members to safeguard their Personal Information consistent with HCA's obligation as a healthcare provider, the promises of which are expressly described herein.

137. Plaintiffs and Class members had agreements with HCA under which HCA agreed to safeguard and protect such information.

138. Plaintiffs and Class members were required to deliver their Personal Information to HCA as part of the process of obtaining services provided by HCA. Plaintiffs and Class members paid money, or money was paid on their behalf, to HCA in exchange for services.

139. Plaintiffs and Class members were required to provide their Personal Information as part of HCA's regular business practices. HCA accepted possession of Plaintiffs' and Class members' Personal Information for the purpose of providing services or Plaintiff and Class members.

140. In delivering their Personal Information to HCA and paying for healthcare services, Plaintiffs and Class members intended and understood that HCA would adequately safeguard the data as part of that service consistent with the express promises herein.

141. HCA breached its express promises to safeguard Personal Information with Plaintiffs and the other Class members by failing to take reasonable measures to safeguard their Personal Information as described herein.

142. As a direct and proximate result of HCA's conduct, Plaintiffs and the other Class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT 4: BREACH OF IMPLIED CONTRACT
On behalf of Plaintiffs and the Nationwide Class

143. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-106 of this Complaint.

144. HCA acquired and maintained Personal Information belonging to Plaintiffs and Class members that HCA received either directly or from its healthcare provider customers.

145. When Plaintiffs and Class members paid money and provided their Personal Information to their doctors and/or other healthcare providers, either directly or indirectly, in

exchange for goods or services, they entered into implied contracts with their doctors and/or healthcare professionals, their business associates, and clinical laboratories, including HCA.

146. Plaintiffs and Class members entered into implied contracts with HCA under which HCA agreed to safeguard and protect such information and to timely and accurately notify Plaintiffs and Class members that their Personal Information had been breached, accessed by an unknown and unauthorized party, and exposed on a hacking forum.

147. Plaintiffs and Class members were required to deliver their Private Information to HCA as part of the process of obtaining services provided by HCA. Plaintiffs and Class members paid money, or money was paid on their behalf, to HCA in exchange for services.

148. Defendant HCA solicited, offered, and invited Class members to provide their Personal Information as part of HCA's regular business practices. Plaintiffs and Class members accepted HCA's offers and provided their Personal Information to HCA, or, alternatively, provided Plaintiffs' and Class members' information to doctors or other healthcare professionals, who then provided the information HCA.

149. HCA solicited, offered, and invited Plaintiffs and Class members to provide their Personal Information as part of HCA's regular business practices. Plaintiffs and Class members accepted HCA's offers and provided their Personal Information to HCA, or, alternatively, provided Plaintiffs' and Class members' information to doctors or other healthcare professionals, who then provided the information to HCA.

150. HCA accepted possession of Plaintiffs' and Class members' Personal Information for the purpose of providing services to Plaintiffs and Class members.

151. In accepting such information and payment for services, HCA entered into an implied contract with Plaintiffs and the other Class members whereby HCA became obligated to reasonably safeguard Plaintiffs' and the other Class members' Personal Information.

152. Alternatively, Plaintiff and Class members were the intended beneficiaries of data protection agreements entered into between HCA and healthcare providers.

153. In delivering their Personal Information to HCA and paying for healthcare services, Plaintiffs and Class members intended and understood that HCA would adequately safeguard the data as part of that service.

154. HCA's implied promise of confidentiality includes consideration beyond those preexisting general duties owed under HIPAA, the FTC Act, or other state or federal regulations. The additional consideration also included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

155. HCA's implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Personal Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized medical purpose; (3) restricting access to authorized, qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the Personal Information against data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

156. Plaintiffs and the Class members would not have entrusted their Personal Information to HCA in the absence of such an implied contract.

157. Had HCA disclosed to Plaintiffs and Class members (or their physicians) that HCA did not have adequate computer systems, information technology security tools, and security practices to secure sensitive data, Plaintiffs and the other Class members would not have provided their Personal Information to HCA (or to their physicians to provide to HCA).

158. HCA recognized that Plaintiffs' and Class members' Personal Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and to the other Class members.

159. Plaintiffs and the other Class members fully performed their obligations under the implied contracts with HCA. HCA breached the implied contract with Plaintiffs and the other Class members by failing to take reasonable measures to safeguard their Personal Information as described herein.

160. As a direct and proximate result of Defendant's conduct, Plaintiffs and the other Class members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT 4: UNJUST ENRICHMENT
On behalf of Plaintiffs and the Nationwide Class

161. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-106 of this Complaint.

162. This count is pleaded in the alternative to any breach of contract claim.

163. Upon information and belief, HCA funds its data security measures entirely from general revenue, including from money HCA makes based upon protecting Plaintiffs' and Class members' Personal Information.

164. There is a direct nexus between money paid to HCA and the requirement that HCA keep Plaintiffs' and Class members' Personal Information confidential and protected.

165. Plaintiffs and Class members paid HCA and/or healthcare providers a certain sum of money, which was used to fund data security via contracts with HCA.

166. As such, a portion of the payments made by or on behalf of Plaintiffs and Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to HCA.

167. Protecting data from Plaintiffs and from Class members is integral to HCA's business. Without Class members' data, HCA would not be able to provide healthcare services, thus compromising HCA's core business.

168. Plaintiffs' and Class members' data has monetary value, and Plaintiffs' and Class members directly and indirectly conferred a monetary benefit on the HCA. Plaintiffs and Class members indirectly conferred a monetary benefit on HCA by purchasing goods and/or services from entities that contracted with HCA, and from which HCA received compensation to protect certain data. Plaintiffs and Class members directly conferred a monetary benefit on HCA by supplying Personal Information, which has value, from which value HCA derives its business value, and which should have been protected with reasonable and adequate data security.

169. HCA knew that Plaintiffs and Class members conferred a benefit which HCA accepted. HCA profited from these transactions and used Plaintiffs' and Class members for HCA's business purposes.

170. HCA enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class members by utilizing cheaper, ineffective security measures. Plaintiffs and Class members, on the

other hand, suffered as a direct and proximate result of HCA's failure to provide the requisite security.

171. Under the principles of equity and good conscience, HCA should not be permitted to retain the money belonging to Plaintiffs and Class members, because HCA failed to implement appropriate, reasonable, and adequate data management and security measures that are mandated by industry standards.

172. Defendant acquired the monetary benefit and Personal Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

173. If Plaintiff and Class members knew that HCA had not secured their Personal Information, they would not have agreed to provide their Personal Information to HCA.

174. Plaintiff and Class members have no adequate remedy at law.

175. As a direct and proximate result of HCA's conduct, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to determine how their Personal Information is used; (iii) the access, compromise, publication, exposure, and/or theft of their Personal Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Personal Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Personal Information, which remain in HCA's possession and is subject to further unauthorized disclosures so long as HCA fails to undertake reasonable appropriate and adequate measures to protect Personal Information in its continued possession; (vii) loss or privacy from the unauthorized access

and exposure of their Personal Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information accessed by an unknown and unauthorized party and exposed as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

176. As a direct and proximate result of HCA's conduct, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm.

177. HCA should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from them. In the alternative, HCA should be compelled to refund the amounts that Plaintiffs and Class members overpaid for HCA's services.

COUNT 6: INVASION OF PRIVACY
On behalf of Plaintiffs and the Nationwide Class

178. Plaintiffs incorporate by reference and re-allege the allegations contained in paragraphs 1-106 of this Complaint.

179. Plaintiffs and Class members have a legally protected privacy interest in their Personal Information, which is and was collected, stored, and maintained by HCA, and they are entitled to the reasonable and adequate protection of their Personal Data against foreseeable unauthorized access, as occurred with the Data Breach.

180. Plaintiffs, Class and Subclass members reasonably expected that HCA would protect and secure their Personal Information from unknown and unauthorized parties and that their Personal Information would not be accessed and disclosed to any unauthorized parties or for any improper purpose.

181. HCA unlawfully invaded the privacy rights of Plaintiffs and Class members by engaging in the conduct described above, including by failing to protect their Personal Information

by permitting an unauthorized and unknown party to access and expose that Personal Information. Likewise, HCA further invaded the privacy rights of Plaintiffs, Class members, and permitted criminals to invade the privacy rights of Plaintiffs and Class members, by unreasonably and by delaying disclosure of the Data Breach, and failing to properly identify what Personal Information had been accessed and exposed by an unknown and unauthorized party.

182. . This invasion of privacy resulted from HCA's failure to properly secure and maintain Plaintiffs' and Class members' Personal Information, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

183. Plaintiffs' and Class members' Personal Information is the type of sensitive information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs' and Class members' Personal Information, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

184. The disclosure of Plaintiffs and Class members' Personal Information to unknown and unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

185. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class members' Personal Information was without their consent, and in violation of various statutes, regulations and other laws.

186. Plaintiffs, the Class and Subclasses members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution, injunctive relief, reasonable attorneys' fees and costs, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 8: FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT,

Fla. State §§ 501.201, et seq.

187. The Florida Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the Florida Subclass, incorporate by reference and re-allege the allegations contained in paragraphs 1-106 of this Complaint.

188. This claim is brought individually under the laws of Florida and on behalf of all other individuals whose Personal Information was accessed by an unauthorized third party and exposed as a result of the Data Breach and reside in states having similar laws regarding deceptive and unfair trade practices.

189. This cause of action is brought pursuant to the Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201 et seq. The stated purpose of this Act is to "protect the consuming public . . . from those who engage in unfair methods of competition, or unconscionable, deceptive, or unfair acts or practices in the conduct of any trade or commerce." *Id.* § 501.202(2).

190. Plaintiffs and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

191. HCA advertised, offered, or sold goods or services in Florida and engaged in trade or commerce directly or indirectly affecting the people of Florida.

192. HCA engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

- (a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Florida Subclass members' Personal Information, which was a direct and proximate cause of the Data Breach;

- (b) Failing to identify foreseeable security and privacy risks and maintain reasonable and adequate security and privacy measures, a direct and proximate cause of the Data Breach;
- (c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Data Breach;
- (d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- (e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. §45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2);
- (f) Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Florida Subclass members' Personal Information;
- (g) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, HIPAA, and Florida's data security statute, F.S.A. § 501.171(2).

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 9: TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT,
Tenn. Code Ann. §§ 47-18-2107, et seq.

193. The Tennessee Plaintiff identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, incorporate by reference and re-alleges the allegations contained in paragraphs 1-106 of this Complaint.

194. This claim is brought individually under the laws of Tennessee and on behalf of all other individuals whose Personal Information was accessed and acquired by an unauthorized third party as a result of the Data Breach and reside in states having similar laws regarding personal consumer information.

195. HCA is business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2). Plaintiff and Tennessee Subclass members' Personal Information include "Personal Information" as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

196. HCA is required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of its data security program in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

197. Because HCA discovered a breach of its computer system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized party, HCA had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

198. By failing to disclose the Data Breach in a timely and accurate manner, HCA violated Tenn. Code Ann. § 47-18-2107(b). As a direct and proximate result of HCA's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, and will continue to suffer damages, as described above.

199. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs request for judgement as follows:

(a) For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class and the Florida Subclass;

(b) For equitable relief enjoining HCA from engaging in the wrongful conduct complained of herein pertaining to the misuse and disclosure of Plaintiffs', Class and Subclass members' Personal Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs, Class and Subclass members, or to mitigate further harm;

(c) For equitable relief compelling HCA to devise and employ appropriate methods and policies with respect to consumer and patient data collection, storage, and protection, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

(d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of HCA's wrongful conduct;

(e) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

(f) For an award of punitive damages, as allowable by law;

(g) Ordering HCA to pay for not less than 10 years of three bureau credit monitoring, identity theft monitoring, and identity theft insurance for Plaintiffs, Class and Subclass members;

(h) For an award of attorneys' fees and costs, and any other expense, including reasonable expert witnesses fees;

(i) Pre- and post-judgement interest on any amounts awarded;

(j) Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 23 day of August, 2023

Respectfully submitted,

/s/ Douglas J. McNamara
Douglas J. McNamara
Blake R. Miller
**COHEN MILSTEIN SELLERS AND
TOLL PLLC**
1100 New York Ave NW, 5th Floor
Washington, DC 20005
Telephone: (202) 408-4600
Facsimile: (202) 408-4699
dmcnamara@cohenmilstein.com
brmiller@cohenmilstein.com

Claire Torchiana
**COHEN MILSTEIN SELLERS AND
TOLL PLLC**
88 Pine Street, 14th Floor
New York, NY 10005
Telephone: (212) 220 2914
Facsimile: (212) 838 7745
ctorchiana@cohenmilstein.com

Steven G. Calamusa
GORDAN & PARTNERS, PA
4114 Northlake Blvd.
Palm Beach Gardens, FL 33410
Telephone: (561) 799-5070
Facsimile: (561) 366-1485
scalamusa@fortheinjured.com

Sidney W. Gilreath
GILREATH & ASSOCIATES, PLLC
550 Maine Ave., Ste 600
Knoxville, TN 37902
Telephone: (865) 637-2442
gilknox@sidgilreath.com

Krysta Kauble Pachman (280951)
kpachman@susmangodfrey.com
SUSMAN GODFREY LLP
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067-6029
Telephone: (310) 789-3100
Facsimile: (310) 789-3150

Vineet Bhatia (00795976)
vbhatia@susmangodfrey.com
SUSMAN GODFREY LLP
1000 Louisiana Street, Suite 5100
Houston, Texas 77002-5096
Telephone: (713) 651-9366
Facsimile: (713) 654-6666

Stephen E. Morrissey (187865)
smorrissey@susmangodfrey.com
SUSMAN GODFREY LLP
401 Union Street, Suite 3000
Seattle, WA 98101
Telephone: (206) 516-3880
Facsimile: (206) 51602883

EXHIBIT A

From: HCA Healthcare <noreply@hcahealthcare.com>

Sent: Sunday, July 16, 2023 6:50 AM

To: [REDACTED]

Subject: HCA Healthcare Privacy Incident



On Monday, July 10, 2023, we announced that a list of certain information with respect to some of our patients was made available by an unknown and unauthorized party on an online forum. The list includes:

- patient name, city, state, and zip code;
- patient email, telephone number, date of birth, gender; and
- patient service date, location and next appointment date.

Importantly, the list does not include:

- clinical information, such as treatment, diagnosis, or condition;
- payment information, such as credit card or account numbers;
- sensitive information, such as passwords, driver's license or social security numbers.

Additional information about the data security incident can be found at hcahealthcare.com/privacyupdate.

We remain committed to protecting the personal information that is entrusted to us. Because patient contact information was involved in this incident, we encourage you to remain vigilant about any suspicious or unexpected communications from an unfamiliar source or from anyone claiming to be affiliated with HCA Healthcare. You can call us at 888-993-0010. Representatives will be available to provide assistance Monday through Friday, 8 am – 8 pm Central Time beginning Monday, July 17. Specifically, if you receive any communication regarding an invoice, outstanding balance, or payment reminder that you were not expecting or believe to be fraudulent, please contact us so that we can confirm the legitimacy of the message.

We are working as quickly as possible to identify and contact patients whose data was impacted by this data security incident. Those individuals can expect to receive a mailed notification letter in the coming weeks and will be offered complimentary credit monitoring and identity protection services.

We appreciate your patience as we continue to work through this event.

Sincerely,
Kathi Whalen
SVP and Chief Ethics and Compliance Officer
HCA Healthcare